2014

The significance of the transition of Supervisory Control and Data Acquisition (SADA) Systems to TCP/IP platforms

Matthew Alexander Care
James Madison University

The Significance of the Transition of Supervisory Control and Data Acquisition (SCADA) Systems to TCP/IP Platforms

A Project Presented to

the Faculty of the Undergraduate

College of Integrated Science and Technology

James Madison University

in Partial Fulfillment of the Requirements

for the Degree of Bachelor of Science

by Matthew Alexander Care

May 2014

Accepted by the faculty of the Department of Integrated Science and Technology, James Madison University, in partial fulfillment of the requirements for the Degree of Bachelor of Science.

FACULTY COMMITTEE:

Project Advisor: Jeffrey D. Tang, Ph.D.,
Associate Dean, CISE

Reader: Timothy R. Walton, Ph.D.,
Associate Professor, Integrated Science and Technology

Reader: Anthony A. Teate, Ph.D.,
Professor, Integrated Science and Technology

Reader: Okechi Geoffrey Egekwu, Ph.D.,
Professor, Integrated Science and Technology

HONORS PROGRAM APPROVAL:

Barry Falk, Ph.D.,
Director, Honors Program

Table of Contents

Acknowledgements

I would like to express my very great appreciation to Dr. Jeffrey Tang and Dr. Timothy Walton for their valuable and constructive suggestions during the planning and development of this research project. I am particularly grateful for the time they sacrificed to meet with me on a regular basis and provide me with the resources that have helped me tremendously. I would also like to extend a special thank you to Dr. Anthony Teate and Dr. Okechi Geoffrey Egekwu for their expertise and guidance throughout the process of producing this project.

Abstract

SCADA system security is a significant United States national security issue based on the systems' vulnerabilities and the cyber threats that seek to exploit them. Within the last fifteen years as SCADA systems have collectively transitioned to Transmission Control Protocol/ Internet Protocol (TCP/IP) networks, analysts and policy-makers have expressed increased concern over the general security and protection of SCADA systems, which are responsible for monitoring and controlling our nation's critical infrastructure. SCADA systems are susceptible based on their ease of entry and their attractiveness as a target. In addition, there a number of cyber threats such as hackers and malware, insiders, terrorist organizations and state actors that are dangerous based on their intent and capabilities. U.S. government engagement with private sector owners and operators of critical infrastructures is essential for mitigating the abundant threats that characterize cyber-terrorism.

Introduction

SCADA Systems

The primary systems associated with the security and facilitation of industrial and facility-based processes are Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems have proven to be popular within critical infrastructure industries such as oil and gas, water, chemicals, electric power, and pharmaceuticals. Their ability to significantly reduce operating costs as well as improve plant or regional system performance and reliability has made SCADA systems an integral part of the utilities industry in the United States since the 1960s.

Purpose

SCADA system security is a significant United States national security issue based on the systems' vulnerabilities and the cyber threats that seek to exploit them. This paper provides a determination and assessment of the consequences of SCADA systems' collective transition to digital Transmission Control Protocol/ Internet Protocol (TCP/IP) networks. In order to answer this question, this report will:

1. Provide a thorough SCADA system assessment including a review of its primary network and control components and an explanation of how these features interact;
2. Determine the nature, characteristics, intents and capabilities of the threats to SCADA systems;
3. Describe the level of ease associated with gaining access to SCADA systems as well as explain the attractiveness of them as a target in order to assess its overall vulnerability;
4. Provide possible solutions that exist to address the problem.

Considering the vital role that critical infrastructure facilities and networks play in society's basic functionality, it is not enough to protect these resources from external entities that threaten them. After production, efforts and costs of a physical system are primarily allocated towards routine supervision and maintenance. For over fifty years, SCADA systems have existed as a technology aimed at making critical infrastructure management efficient. The data collection capabilities of SCADA systems within a facility or dispersed location eliminate personnel from spending time physically inspecting facilities and performing maintenance, thus minimalizing field site examinations. Costly after-hours and alarm call-outs can often be avoided since a SCADA system will indicate the nature and degree of a problem. The ability to remotely control site equipment may permit an operator at home to postpone a site visit till working hours.[1] Additionally, such systems possess a very reliable alarming system that relays critical data immediately to process control, which allow informed network system decisions to be made.

SCADA systems are easy to manipulate and control, largely because of their intuitive interfaces and reliable speed. When graphically displayed, accumulated operating data will often indicate a developing problem or an area for process improvement.[2] In addition, SCADA systems can often be accessed remotely through an internet connection on one's computer, laptop, phone or tablet, depending on the capabilities of any particular system. SCADA systems feature an array of advantages that have increased their popularity and usage over time. Their versatility and effectiveness make them an essential component of any industrial control system.

Despite the enhanced capabilities brought forward by the development of technology relating to SCADA systems; this progress has not come without a number of serious security

[1] SCADA explained. (2012). *Opus Daytonknight,*
[2] SCADA explained. (2012). *Opus Daytonknight,*

concerns. Newly introduced, internet-connective capabilities of SCADA systems have been identified as the systems' primary security concern, amongst many others. Before the transition to TCP/IP digital platforms, SCADA systems lacked Internet capabilities that enabled networking and interconnectivity between various systems, making protective features unnecessary. However, this new function has created a channel through which various cyber-based threats could emerge and infiltrate the security of the systems. Additionally, many SCADA systems that were not immediately supported by necessary cyber-security features such as firewalls, routers or anti-virus software created a considerable national security issue for government leaders and private-sector ownership alike.

Within the last fifteen years, analysts, national security leadership and policy-makers have expressed increased unease over the general security and protection of critical infrastructure systems because of the number of significant threats that currently accompany SCADA systems' security weaknesses. These threats include but are not limited to malcontented insiders, hackers, terrorist organizations and state actors. The vulnerability of the SCADA systems and the attractiveness of a critical infrastructure targets that they administer in combination with the intent and capabilities of the previously described threats collectively merit substantial attention from our nations' security leaders.

Technical Overview

Understanding the Technical Characteristics of SCADA Systems

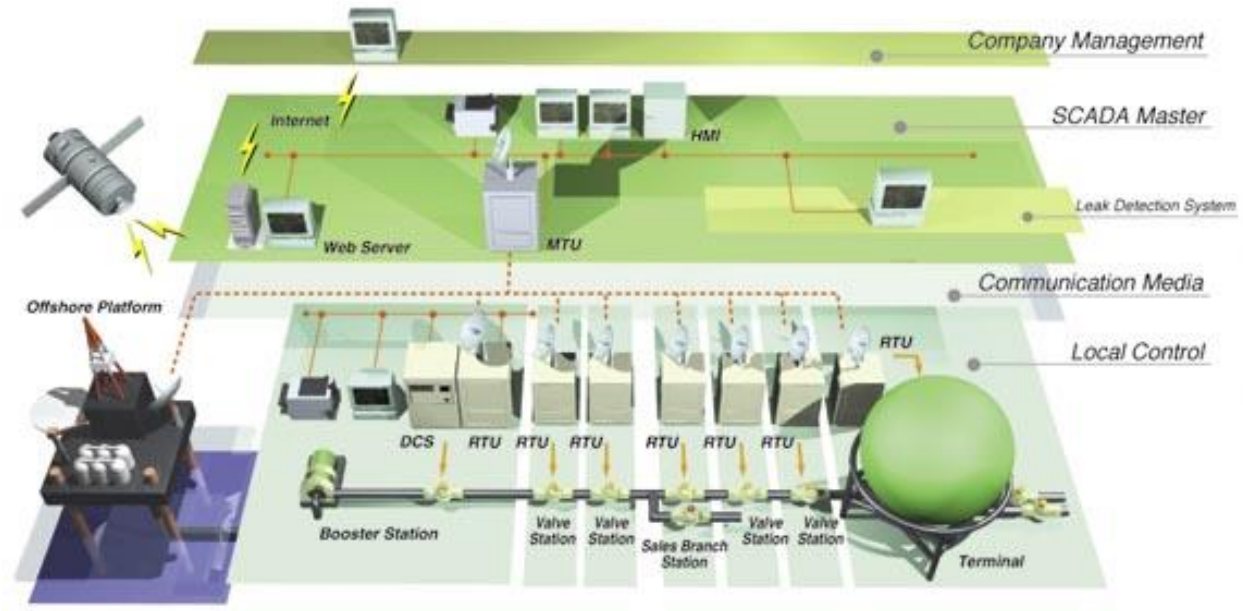

Figure 1: The primary components of a SCADA system.[3]

Industrial Control System (ICS) is a term that is used to refer to multiple types of control systems used in the industrial sector and critical infrastructure such as SCADA systems, distributed control systems (DCSs) and programmable logic controllers (PLCs). SCADA systems are highly dynamic arrangements that are used to secure and centrally collect data on critical infrastructure networks that are oftentimes geographically dispersed. These systems assimilate hardware and software to provide a centralized monitoring and control center that features both input and output functions.

[3] What is a SCADA system. (2005). Retrieved 12/8, 2013, from http://www.veestaworld.com/pages/services_scada_pages.htm

In order to understand a SCADA system's functionality, it is vital to become familiar with the major control components of a common industrial control system.

Control Components:

- Master Terminal Unit (MTU): Operating as a component of the SCADA master level; the MTU acts as the central processing unit of the entire system. The MTU controls the actions of all of the local control units such as the Remote Terminal Units (RTUs) and the Programmable Logic Controllers (PLCs) in addition to the dynamic control functions that are completed both automatically and by an operator.
- Remote Terminal Unit (RTU): "RTUs are field devices that are often equipped with wireless radio interfaces to support remote situations where wire-based communications are unavailable with the purpose of data acquisition and unit control.[4]" Along with PLCs, RTUSs are the primary technical components of the field level areas that cover the systems' physical scope and are vital to transmitting data to the master system.
- Programmable Logic Controller (PLC): Like remote terminal units, PLCs are responsible for executing many of the same data acquisition and field level maneuvers. In SCADA environments however, PLCs are designed for specific control applications and are therefore used often as field devices because they are more economical, versatile, flexible and configurable than special-purpose RTUs.[5]
- Human-Machine Interface (HMI): A HMI is a critical hardware and software element that allows human operators to influence and interfere with the system based on company management and decision-making. "The connection between the SCADA master level

[4] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[5] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.

and company management allow for operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency.[6]" This interface also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users[7].

- Intelligent Electronic Devices (IED): An IED is a field sensor that is used to acquire data and perform control functions in conjunction with other functions at the local control level. "An IED can combine an analog input sensor, analog output sensor, low-level control capabilities, a communication system and program memory in one device.[8]" These features allow greater interconnectivity and advanced communications capabilities at the local level.
- Data Historian: A systems' data historian is a database software application that serves to record time-based process data. Typically, historian software offers the features of trending software (which includes managing basic system information) with enhanced data capturing, data compression, and data presentation capabilities.[9]
- Input/Output (IO) Server: A SCADA systems' IO server is responsible for processing the data that is transmitted from the primary components of the local control locations via communication media. An IO server can reside on the control server or on a separate

[6] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[7] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[8] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[9] IHS Global Spec.Trending and historian software information. Retrieved November 26, 2013, from http://www.globalspec.com/learnmore/industrial_engineering_software/industrial_controls_software/trending_historian_software

computer platform. IO servers are also used for interfacing third-party control components, such as HMI and a control server.[10]

Network Components:

- Communication Network: The fieldbus network is a collection of industrial computer networks that enable communication with a PLC. The fieldbus network distributes information uniformly to the various field sensors using a specific procedure that eliminates narrow sensor-to-sensor interaction.
- Control Network: The control network establishes interconnectivity amongst the control levels that comprise the system such as the SCADA master level and the local control level.
- Communication Router: A router is a communication media device that enables interaction between two control networks, including local area networks (LAN) and wide area networks (WAN). In a SCADA system, this connection is between the Main Terminal Unit and the Remote Terminal Units to the control network for SCADA communication.
- Firewall: A firewall exists to protect network communication by scanning and controlling network communications.
- Modems. A modem is a device used to convert between serial digital data and a signal suitable for transmission over a telephone line to allow devices to communicate. "Modems are often used in SCADA systems to enable long-distance serial communications between MTUs and remote field devices.[11]"

[10] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[11] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.

- Remote Access Points: Remote access points are distinct devices, areas and locations of a control network for remotely configuring control systems and accessing process data. Examples include using a personal digital assistant (PDA) to access data over a LAN through a wireless access point, and using a laptop and modem connection to remotely access an ICS system.[12]

Understanding the Interactive Functions of a SCADA System

SCADA systems feature relationships between several vital control and network mechanisms that operate together in unison in order to control and collect data on network operations. Because these systems are used in delivery systems that span over broad physical areas such as water, oil and electrical distribution systems, the importance of having strong network connectivity is high.

SCADA Hardware and Software

Today, the common SCADA system consists of user operation workstations, SCADA server computers, communication networks, programmable field controllers and field devices and signals. "Typical hardware includes a master terminal unit placed at the control center, communications equipment (e.g. radio telephone line, cable, or satellite), and one or more geographically distributed field sites consisting of either a remote terminal unit or a programmable logic controller.[13]" Functionally, the remote terminal units and programmable logic controllers gather specific data about the network structure that it monitors (such as where

[12] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[13] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.

a leak on a pipeline has occurred) and records the data as unique. The data is then transitioned through the input/output server (communication hardware) to a central command site where the master terminal unit is located where it stores and processes the information. The system ultimately alerts the home station that a leak has occurred by carrying out necessary analysis such as determining the critical characteristics of the situation. This information is presented in a clear and organized layout, providing supervisors with actionable intelligence. Graphic 2 illustrates the basic architecture of a SCADA system.

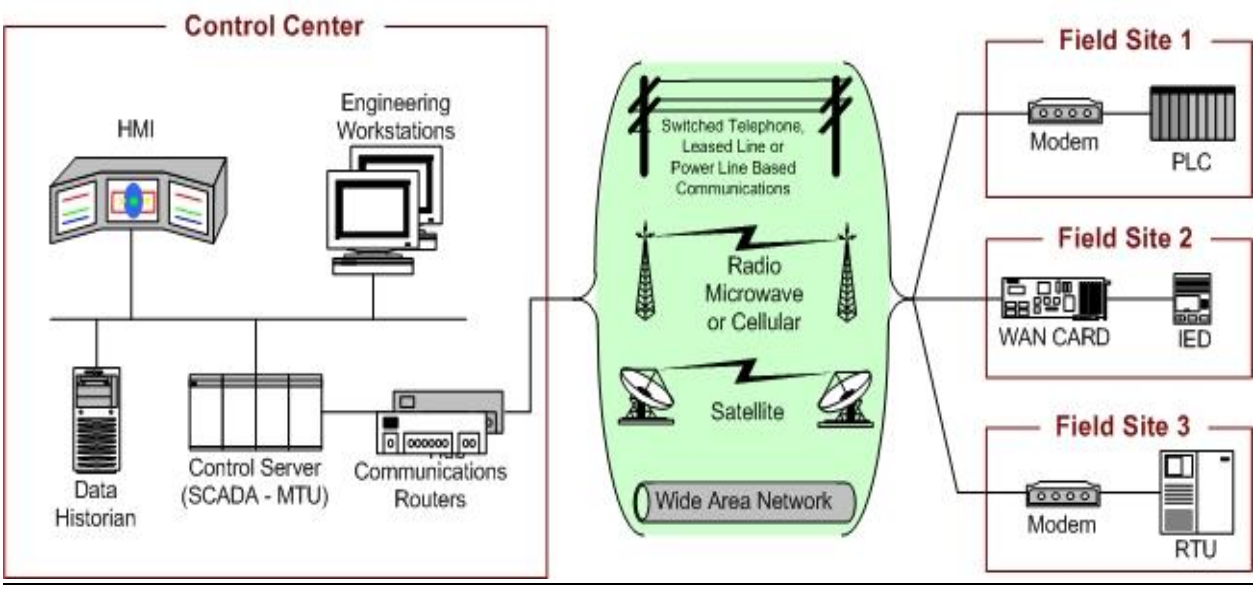

Figure 2: The connection between the control center and the multiple field sites at the local level.[14]

These functions are controlled through the SCADA software and network components. The network features are mostly uniform throughout most industrial control systems and include many of the devices that were outlined previously such as the communication router, the control network, and the remote access points. However, a systems' software is unique, with respect to not only the type of industrial control system that it is employed in such as water, power or

[14] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.

electric, but also each SCADA system specifically. Each system has its own specific architecture and functionality, and these elements must be considered in the software creation stages. However, there are baseline software functions that are programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate when parameters change outside acceptable values.[15] These principles apply to the software of the five basic components of any SCADA system architecture.

SCADA System Architecture

Field devices and signals are the portals through which data is transmitted in or from the PLC in either a discrete form or an analog form. Their function in relation to the other signals and devices must be considered when designing the system software. Field devices may be signal transmitters, such as level or pressure transmitters; they could be discrete signals, such as a valve's open or closed status or the motors' running status. "Some devices may actually provide multiple signals, such as a water quality unit, which provides both chlorine residual and water pH. [16]" Once all of the field signals have been identified for each of the process areas, the connections can be made through the SCADA software.

A SCADA system is divided into multiple process areas that have their own function to be executed. Each one of these locations require a PLC or RTU that executes data acquisition and field level maneuvers. For example, "a pumping station may use two or three pumps, operating in a lead/lag/standby mode; the automation program in the controller is configured to operate the pumps based upon operator-entered setpoints and duty assignments that are executed

[15] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[16] McCrady, S. (2013). The elements of SCADA software. Designing SCADA application software: A practical approach (pp. 11-23)

through the programmable logic controller.[17]" After the software designer allocates the proper I/O signals to each PLC, organizing them according to input/output and discrete/abstract the system will be ready for communicative functions at the local control level.

The human machine interface, or the user workstation, is the graphic display that allows for an operator to control system functionality and control data acquisition. The software at this level involves the creation of the process control displays, historical trend and historical report displays, alarm and event summary displays, and the process database.[18] This can be established through the programming of the graphic displays associated with the links in the process database as well as the programming of the communications interface for the RTUs and the PLCs.

The communication network for a SCADA system connects the SCADA master/company management level with the various local control levels that are spatially dispersed. The three basic topologies for communication networks as they pertain to SCADA systems include bus, star, and token ring networks.[19] While all of these networks connect the essential nodes of the SCADA together in their own way, they all serve the same connective function; albeit each method of communication is used depending amount and importance of the data being transmitted. Having a secure communication network is essential in order to ensure that the control and network functions cannot be interrupted externally.

The SCADA server computer is the system device that maintains all communicative and data acquisition functionality. Historical data collected over time is maintained on the server

[17] McCrady, S. (2013). The elements of SCADA software. Designing SCADA application software: A practical approach (pp. 11-23)
[18] McCrady, S. (2013). The elements of SCADA software. Designing SCADA application software: A practical approach (pp. 11-23)
[19] McCrady, S. (2013). The elements of SCADA software. Designing SCADA application software: A practical approach (pp. 11-23)

computer in the form of databases. Current system operating data from all of the field controllers is also maintained in databases on the server computer.[20] This historical data is continuously updated with new data that is acquired via communications with the PLCs and the RTUs, which is ultimately a function made through the server computer. Another purpose of the SCADA server computer is to provide an interface to other facilities, typically through the Internet, using firewalls and SQL interface calls. "It is important that the outside access cannot interfere with the internal operations of the SCADA system, so the server computer often provides a secure interface.[21]" It is through the server computer that interconnectivity amongst various facilities accomplishes data sharing and other interactive features.

Ultimately, all of these components combine to create an industrial control system that is able to monitor and control industrial processes while including multiple sites over long distances. Identifying the primary control and network components that comprise the makeup of SCADA systems allows for a fundamental understanding of the system itself, which in turn enables a more comprehensive view of what vulnerabilities exist within the system and how they can be exploited.

[20] McCrady, S. (2013). The elements of SCADA software. Designing SCADA application software: A practical approach (pp. 11-23)
[21] McCrady, S. (2013). The elements of SCADA software. Designing SCADA application software: A practical approach (pp. 11-23)

Threat Analysis

American National Security – A Broad Overview

According to Clark Kent Ervin at the Aspen Institute, terrorists remain fixated on an aviation-style attack, with the intention of inspiring fear in American citizens that permeates down to the most basic levels of society. While we remain vulnerable in the aviation sector, it remains our strongest area of security. Therefore, if a successful attack were implemented on our airplanes, it would be evident that the United States is vulnerable, even at its strongest area. However, with our improved technology and public awareness, it will be very difficult for terrorists to execute an attack similar to the one that was launched against the American people on 9/11.

Figure 3: 9/11 reminds us why strong national security is vital.

Air cargo, is an extreme concern, because it goes through far less extensive screening compared to carry-on and passenger luggage. Right now, explosives are the chief concern among national security representatives yet TSA representatives constantly scan for guns and knives as well. Maritime cargo presents a far larger threat as only 5% of maritime cargo containers are inspected for radioactive materials. Mass transit also remains a large threat based on the nature of American transportation in that 85% of critical infrastructure in the U.S. is privately owned and operated by those who may value profit over security. It would be advantageous for the government to collaborate with these private companies in order to ensure greater security because the products and services produced by private firms are not limited by government regulations.

Finally, the status of America's national security is concerning for a number of reasons. First, the geographic dimensions of the United States present inevitable limitations to those in charge of overseeing our national security based on the size of our borders. Second, the importance of intelligence and national security is illuminated through these vulnerabilities in part because Americans tend to be more reactive than proactive. Third, biological and chemical weapons remain an issue – very little technology has been developed to detect them. Fourth, resources in the tight budgetary times of 2014 prevent the United States from implementing the proper actions and purchases necessary to build our national security to protect against various threats. Fifth, both northern and southern borders remain extremely vulnerable as evidenced by the number of illegal aliens that come into the U.S. with ease. Sixth, the same principle of unavoidable limits mentioned earlier can be applied on a case by case basis when it comes to situations where action could have been taken to prevent a possible attack, yet none was taken. For example, before 9/11 had occurred, one of the hijackers who would eventually become

involved in the attack had taken flight lessons in order to learn how to operate a plane. During these lessons, the man was not interested in learning how to land the plane. The instructor thought this was odd, yet did nothing in the way of altering authorization. This is an example of this principle of inevitable limitations. In the event of a designed terrorist attack, there are simply too many acts that have to be prevented over the course of time. Despite all of these threats to American national security, it seems that the most alarming threats to the United States in regards to terror lies on the cyber battlefield, where serious damage could be inflicted on our critical infrastructure.

Cyber Terrorism

Industry, finance, intellectual property, technology, culture, policy and diplomacy are some of the many areas in which the United States has become dependent on the cyber domain.[22] The functionalities of the cyber domain include the creation, transmission and utilization of digital information. "Voice, video and data communications are transmitted through wired and wireless mediums to a range of connected devices that can include desktop and laptop computers, smart phones, mainframes, televisions, radios, supervisory control and data acquisition (SCADA) systems, sensor and navigation systems and communication satellites.[23]" This empowers global communication and information-sharing to occur, which in turn facilitates the evolution of capabilities in nearly every aspect of life. This communication comes in the form of digitalized content, digital devices and services and telecommunications, which forms an increasingly interdependent cyber domain. Obviously, the United States has an extremely large

[22] Kahn, R., McConnell, M., Joseph, N., & Schwartz, P. (2011). America's cyber future.
[23] Kahn, R., McConnell, M., Joseph, N., & Schwartz, P. (2011). America's cyber future.

digital footprint within the cyber sphere that transcends international boundaries and potential language barriers.

Cyber terrorism can be defined as: "the use of computers as weapons, or as targets, by politically motivated international or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies.[24]" Ever since the early 1990s and early 2000s, cyber-based threats have been recognized by analysts as "the next big threat to American national security," or "the looming threat over the horizon." Before 9/11, a number of exercises identified apparent vulnerabilities in the computer networks of the United States military and energy sectors, which raised a moderate level of apprehension. Following the events of 9/11, the security and terrorism discourse soon featured cyber terrorism prominently, promoted by interested representatives of the political, business and security circles.[25] Cyber terrorism has now undoubtedly become a global defense issue that governments around the world have to account for.

Foreign agents are attempting to expose the vulnerabilities of the national security of the United States. Americans themselves, as well as foreign adversaries, have identified the realm of cyber security as a potential weak spot for the United States.[26] This exposure exists for a number of reasons, but perhaps the most profound evidence of this lies in the United States' growing dependency on the information technology (IT) that supports nearly all aspects of American society. "Data collection, processing, storage and transmission capabilities are increasing

[24] Wilson, C. (2005, April 01). *The navy department library*. Retrieved from http://www.history.navy.mil/library/online/computerattack.htm
[25] Weimann, G. (2004, May). *United states institute of peace*. Retrieved from http://www.usip.org/publications/cyberterrorism-how-real-threat
[26] Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: Director of National Intelligence, Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: (2012).

exponentially; meanwhile mobile, wireless and cloud competing bring the full power of the globally-connected Internet to a myriad of personal devices.[27]" Despite all of the improvement and innovation of the capabilities of technology and network systems, this progress has outstripped advancements in security. Neither the public nor the private sectors have emphasized enough focus into the implementation of proper security measures. The threat of a cyber-attack is recognized in the intelligence community as considerable based on the nature, scope, and potential for disarray that characterizes cyber-security incidents, as well as the range of actors and targets involved.

Perhaps the most concerning aspect of the emerging threat of cyber-terrorism is the potential for an attack to be launched on network systems that would affect American critical infrastructure. "Critical infrastructure is defined as the assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.[28]" This can include but is not limited to electricity generation, gas production, oil production and distribution, transportation (railroads, highways, airports, ports, inland shipping), public health facilities (hospitals, ambulances), food production, water supply (drinking water, sewage), telecommunication, security services (police, military) and heating (natural gas, fuel). These resources serve as the backbone of any country; but in the United States, a nation with well over 300 million people, critical infrastructure plays a particularly indispensable role especially considering the America's dependency on technology.

[27] Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: Director of National Intelligence, Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: (2012).

[28] Critical infrastructure sectors. (2014). Retrieved 4-16, 2013,

The challenge of a cyber-based national security breach is not a new one for the United States, but the elevated threat towards the nation's critical infrastructure is. The enhancement of computer literacy and technological capabilities has ushered in better competency in hackers, terrorist organizations and adversarial nation-states. Perhaps the most plausible approach a challenger may take when aiming to negatively influence the function of American critical infrastructure is through the infiltration of SCADA systems. Additionally, a number of vulnerabilities within the systems have been identified as significantly concerning.

Ultimately, the current security status of SCADA systems illuminates and uncovers a striking national security liability. Combine this factor with the potential impact of an attack on American critical infrastructure, and it becomes increasingly apparent that the United States must find a way to mitigate the threats and weaknesses that exist to potentially cause harm to the backbone of the country. This report will examine such threats and vulnerabilities to the critical infrastructure system within the United States in order to determine the prospective impact that an attack could have.

Significant Threats to SCADA System Security

Ever since critical infrastructure made the transition to TCP/IP platforms, numerous threats have been identified as significantly problematic by intelligence analysts and policy-makers. Malware can introduce SCADA systems to viruses, worms, Trojan-horse attacks, and spyware. Insiders such as disgruntled workers can pose a very substantial threat to any sensitive system, based on the person's easy accessibility to both physical and digital areas of the system and their ability to manipulate it in a way that an outsider may not be able to. Hackers also present noteworthy security risks through their interest in probing, intruding or controlling a

system because of the challenge it presents. Lastly, terrorist organizations and state actors are threats to United States' critical infrastructure and SCADA systems based on their greater capabilities through access to resources and bolder intent driven by potentially anti-American ideologies.

These five threats can be explained by conducting an analysis that examines all of the available information concerning potential adversaries in conjunction with its intent and capabilities.

Hackers and Malware

The process of hacking refers to someone breaking into a computer or network, usually by exploiting an existing flaw.[29] Malware is an abbreviated term meaning "malicious software," and refers to software that is specifically designed to secretly access one's computer, or server, and compromise its main functions, steal data, bypass access controls or otherwise harm the computer.[30] It is important to understand the relationship between these two terms because they are central towards identifying the different types of attacks that one could encounter through the Internet. Malicious hacking is an action that is primarily represented by those that are driven by the desire for profit, protest, or challenge, and has spawned a subculture of individuals that are drawn to its characteristics. As computer science has evolved, so too have the capabilities of malicious software which has primarily been developed and disseminated by those in the hacking community who are known as "black hats." Malware has largely been the apparatus through which hacking has operated since its inception, which includes multiple motives behind

[29] Hacking, phishing and malware...OH MY. (2014). Retrieved 2/24, 2014, from https://www.liquidweb.com/blog/index.php/hacking-phishing-and-malware-oh-my/
[30] Hacking, phishing and malware...OH MY. (2014). Retrieved 2/24, 2014, from https://www.liquidweb.com/blog/index.php/hacking-phishing-and-malware-oh-my/

its use itself. Malware can be used to hack into a network or system in order exploit vulnerabilities or acquire data, or it can be used to simply inflict damage to another computer for no real reason. To understand malicious hacking, is to understand malware.

Like any IT system, SCADA systems are potentially vulnerable to viruses, worms, Trojans and spyware. This may be the only identified threat that could be characterized as indirect and therefore potentially unintentional attack; however it could still very well impact the system by corrupting data, overwhelming communications, installing back doors or key stroke loggers. Although this is a negative element that could be presented by a hacker or other adversarial agent, it is not uncommon to see malicious software accidentally introduced by employees who unknowingly connect flash drives that are not compatible with the SCADA system software or contain harmful files of their own. Regardless of whether or not malicious software is embedded in a system directly or incidentally through various backchannels, malware original design was created with the goal of destruction and manipulation in mind making it a constant and serious threat.

The primary elements behind intent include both desire and expectation. In the case of routine malicious software, the elements that comprise intent take on a different meaning based on the fact that the malware program has no control over any specific target program. Instead, the input of the target program is taken over by the malicious outputs from the malware's program. "The malware programs' outputs are referred to as attack goals which are divided into two different types of security attacks: memory-based (such as buffer overflow or format string attacks) and function-call-based attacks.[31]" Function-call-based attacks generally comprise the focus of cyber-attacks because they produce hostile actions directed at the target program or system. "Most of today's viruses, worms, Trojans, backdoors, Denial of Service (DoS) tools and

[31] Shin, J., & Spears, D.The basic building blocks of malware.

other hacking tools that are written in high-level computer languages such as C/C++ are function function-call-based attacks that involve malevolent actions such as opening a TCP port to send a copy to itself to remote machines, dropping a backdoor, deleting or interception sensitive information, modifying system configurations of the victim's machine, and so on.[32]" Defining the key terminology of the various types of malicious software is a critical component towards understanding what it is generally capable of:

- Viruses: "A computer program that is usually hidden within another seemingly innocuous program and that produces copies of itself, inserts them into other programs, and usually performs a malicious action such as destroying data.[33]"
- Worms: In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. "A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.[34]"
- Trojan Horse: Users are typically tricked into loading and executing it on their systems. "After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses).[35]"

[32] Shin, J., & Spears, D.The basic building blocks of malware.
[33] Distler, D.Malware analysis: An introduction. *SAN Institute Reading Room,* Retrieved from http://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103
[34] What is the difference: Viruses, worms, trojans, and bots? (2014). Retrieved 2/20, 2014, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html
[35] What is the difference: Viruses, worms, trojans, and bots? (2014). Retrieved 2/20, 2014, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

- Spyware/Adware: Software that is installed in a computer without the user's knowledge and transmits information about the user's computer activities over the internet, or through targeted advertisements.[36]
- Backdoors: A backdoor is an undocumented way of accessing a system, done by bypassing the normal authentication mechanisms. "Usually attackers use backdoors for easier and continued access to a system after it has been compromised.[37]"
- Bots: A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their targets.[38]

Based on the danger that malware can present to any program, it is vital to protect SCADA systems from this type of threat. Malware designers employ various motives when they set out to distribute harmful software throughout cyberspace. The incentive for such an act originated as experiments and pranks but the black-hat community has evolved towards the deliberate destruction of targeted programs and systems. Today, much of malware is created for profit through forced advertising (adware), stealing sensitive information (spyware), spreading email spam or child pornography (zombie computers) or extorting money (ransomware).[39] By analyzing the outputs of a malicious program, it is clear that malware is created with the intent to

[36] Distler, D.Malware analysis: An introduction. *SAN Institute Reading Room,* Retrieved from http://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103
[37] What is the difference: Viruses, worms, trojans, and bots? (2014). Retrieved 2/20, 2014, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html
[38] What is the difference: Viruses, worms, trojans, and bots? (2014). Retrieved 2/20, 2014, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html
[39] What is malware and how can we prevent it? (2010). Retrieved 2/20, 2014, from http://www.pctools.com/security-news/what-is-malware/

corrupt a computer's functionality and has manifested in the form of malware and assorted cyber-attacks. Considering the dynamic and dangerous capabilities that characterize malware, the threat that malware pose to SCADA system is considerable.

In light of the threat that malware pose to various networks and systems, it is vital to understand the culture of hacking. Black-hat hackers are not only the developers and the disseminators of malicious software across cyberspace, but they are most importantly the enablers. Without hackers, malware might only exist as a routine nuisance for computer users. Although the hacking community is certainly not uniform, it seems that it is bound by many of the same characteristics that define the counterculture, but obviously includes a focus on information and communication technologies. The malicious hacker profile might generally be characterized by a person who is involved in countercultural activism with some type of political commitment and is fascinated with the opportunities afforded by the world of hacking and programming.[40] Whether it is through spreading viruses, cracking software or manipulating networks, the hacking community is united and collaborative across its various subcultures, no matter the motivation. Certain hacking cultures are driven by political and or cultural ideology; some hack for financial gain and others do so for sport. Yet, this culture is a loosely networked collection of subcultures that is nevertheless conscious of some important shared experiences, shared roots, and shared values.[41]

In relation to SCADA systems and critical infrastructure protection, the computer hacker remains a serious threat. Recently an article in *The Washington Times* reported that the Department of Homeland Security (DHS) is warning that hackers from the loose online protest

[40]Spilker, H.Punks, hackers, and unruly technology. *Media and revolt: Strategies and performances from the 1960s to the present* ()

[41] The jargon file: Hacker slang and hacker culure. Retrieved 2-27, 2014, from http://www.catb.org/jargon/html/introduction.html

collective called Anonymous have threatened attacks against the computer systems that run factories, power stations, chemical plants, and water and sewage facilities.[42] The statement goes on to warn that SCADA systems are considered amongst the most the attractive targets for hackers and that they "could be able to develop capabilities to gain access and trespass on industrial control system networks very quickly.[43]" Compared to the other primary cyber threats against SCADA systems, the hacking community is much more individualistic and isolated. While not all hackers share identical or even similar objectives or capabilities, it important to recognize there is a small percentage of hacking community that does have the intent and resources to potentially inflict serious harm on SCADA system networks which could impose serious harm on SCADA networks.

Insiders

An insider can be defined as a disgruntled employee, contractor or business partner that could potentially use his or her privileged knowledge to exploit a particular system they have access to. The insider may be motivated to damage or disrupt a SCADA system or the utility's physical system based on the desire to gain higher privileges, displeasure with organizational decision-making or salary-based frustration. Insiders can obtain a great deal of knowledge about computer intrusions because their understanding of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data.[44] A resentful individual who knows the system can potentially be the most significant threat to any kind of

[42] Waterman, S. (2011). Hacker group threatens industrial computer systems. Retrieved 2-12, 2014, from http://www.washingtontimes.com/news/2011/oct/17/hacker-group-threatens-industrial-computer-systems/
[43] Waterman, S. (2011). Hacker group threatens industrial computer systems. Retrieved 2-12, 2014, from http://www.washingtontimes.com/news/2011/oct/17/hacker-group-threatens-industrial-computer-systems/
[44] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.

system, based on the person's easy accessibility to the software and ability to manipulate it. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.[45] The threat level of an insider exploiting a SCADA system is dependent on a case-by-case basis. Although the motivation to commit a deliberate insider attack is often not enough to influence an individual to act, the knowledge and resources available to various employees, contractors or business partners makes an insider attack an ever-present and dangerous possibility.

Terrorist Organizations

The goal of terrorism is to inconvenience and inspire fear, not simply to kill a significant amount of people. This can cause a daily, corrosive effect on the way a society operates by influencing the basic decisions one could make in a day. Organized terror manifested strongly during the Clinton presidency with the 1993 World Trade Center bombings in New York, including related conspiracies; the 1996 Oklahoma City bombing; the 1998 East Africa bombings; and the Tokyo sarin-gas attack in 1995.[46] Over the course of roughly the last two decades, a new wave of religiously-motivated terrorism has accompanied the old standard of state-sponsored terrorism. Specifically, terrorist organizations founded on Islamic extremist principles such as al-Qaeda, Hamas and the Taliban have spread violence and intimidation globally since in the late-1980s. U.S. analysts believe that religiously motivated terrorism will persist for many years and that its Islamic manifestation will remain a threat regardless of what occurs to the respective leaders of each organization.[47] Today, American society has become

[45] Stoufer, K., Falco,J., & Kent,K.Guide to supervisory and data acquisition (SCADA) and industrial control systems security.
[46] Benjamin, D., & Simon, S. (2000). America and the new terrorism. Survival, 42(1), 59-75.
[47] Benjamin, D., & Simon, S. (2000). America and the new terrorism. Survival, 42(1), 59-75.

increasingly vigilant of the characteristics of Islamic terrorism as a result of the 9/11 attacks and the more recent Boston Marathon bombing. Likewise, the US government has recognized the shift from state-on-state military action to the emergence of the terrorist threat as evidence of the immense amount of resources that have been devoted towards security across a multitude of applications.

In order to understand the intent that terrorist organizations pose against SCADA systems, becoming familiar with the nuances that characterize Islamic theology with extremist ideology is critical. Jihadi Salafist, or Islamic extremism, is represented by a small sect of the Muslim religion that believes in a strict interpretation of the Tawhid and Jihad theological ideology. In mainstream Islam, Tawhid is a "doctrine of oneness" that asserts that there is only one god, he only has no partners meaning that only he has the right to be worshiped, and anyone who worships another god is sinning. Conversely, Islamic extremism interprets that anyone who even claims to have sovereignty or makes laws is making himself into a god and must be killed. This is why al-Qaeda and the Taliban are moved to use violence to achieve their political objectives. Moreover, these terrorist organizations have promoted the idea of wala' wa'l-bara'a which refers to an Islamic alliance and disavowal specific to extremism; that only those who agree fully with their ideology is truly Muslim, thus those who do not are disinherited and can be killed without prosecution. Today, jihad is commonly understood as an internal struggle and defensive war in order to establish a just society. Conversely, terrorist extremists interpret this notion as an individual duty that is a personal matter for each individual with a focus towards waging war against the impurities of society, namely other Muslims that do not align with their line of thought. This explains why for every on non-Muslim killed, eight Muslims are.

For al-Qaeda specifically, their objectives consist of a number of incremental steps they believe will result in a just global society:

- Remove non-Muslim occupiers and the current "apostate" rulers.
- Impose their version of Shari'a law.
- Set up emirates (governments) under their ideology.
- Create the caliphate, or governing body. Without this in place, everyone is living in sin.
- Make god's word the highest; achieved through conquering the world and forcing everyone to align with Islamic extremism.

The means towards these goals include:

- Attack America and its allies.
- Fight the jihad in order to impose their Shari'a law.
- Unify the jihad.
- Incite and coalesce the Ummah (the Islamic unity).
- Command right and forbid wrong: the only thing one is allowed to do is live the extremist life.

The mission of al-Qaeda, like other extremist terrorist groups, is a global one. To these groups, the U.S. is not at the center of their objectives. The events of 9/11 made most Americans believe that al-Qaeda was and still is driven by destruction of America and her allies. Instead, al-Qaeda's goals include overthrowing the current governments and establishing Islamic emirates, with the ultimate objective of creating a "caliphate" government that would be about Islamic extremism and would chiefly reign over what currently constitutes the current Muslim world that spans across the Middle East, South and Central Asia, Africa, and southern Europe. Of course,

the destruction of the United States remains a very high priority across different terrorist leadership. Based on evidence collected in Afghanistan, al-Qaeda has a "high level of interest" in DC and SCADA devices.[48] From an intent-related perspective, it is unlikely that there is a malicious entity that desires to tear down the United States more than the leading terrorist organizations. Therefore, critical infrastructure is and will continue to remain a leading attractive target for terrorist leadership going forward based on not only the collateral damage that an attack would have, but also the immense fear that it could potentially impose.

Considering the motivation to attack the United States that define terrorist agenda, it is vital to understand the primary capabilities across these extremist organizations, specifically in the cyber realm. This is the threat that distinguishes critical infrastructure from most IT systems. A terrorist organization is likely to seek to disable the SCADA system to disrupt its monitoring and control capability, take control of the system to feed false values to the operators or use the control system to degrade service or possibly damage the physical critical infrastructure system.[49] For national security officials, part of understanding and preparing for such a possibility includes identifying what terrorist organizations are capable of in cyberspace. Although there have been no major cyber-attacks caused by groups that have taken lives or caused severe physical destruction, some government experts believe that terrorists are at the point where they may be able to use the Internet as a direct investment to cause casualties, either alone or in conjunction with a physical attack.[50] Digging deeper, U.S. security agencies are able to analyze the cyber activity of terrorist organizations in order to anticipate where and how an

[48] Hildick-Smith, N. (2005). Security for critical infrastructure scada systems. Retrieved from http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644
[49] Hildick-Smith, N. (2005). Security for critical infrastructure scada systems. Retrieved from http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644
[50] *Critical infrastructure: Threats and terrorism.* (10 August 2006). (Handbook No. 1.02). Fort Leavenworth, Kansas: Deputy Chief of Staff for Intelligence (DCSINT). Retrieved from http://www.fas.org/irp/threat/terrorism/sup2.pdf

attack could be carried out. "The discovery in Afghanistan of a computer containing structural analysis programs for dams, combined with an increase in Web traffic relating to SCADA systems, prompted the National Infrastructure Protection Center (NIPC) to issue a warning information bulletin.[51]" An analysis of cyber-attack data collected during the second half of 2001 showed that the corporate systems of energy industry companies are attacked twice as often as other industries, and that a large number of these attacks originate from the Middle East.[52]

As the emphasis for cyber-related capabilities have increased exponentially in recent years, intelligence continues to suggest that the technical capabilities of members of terrorist organizations are increasing. "A recent study of more than 200,000 multimedia documents on 86 sample websites concluded that extremists exhibited similar levels of web knowledge as U.S. government agencies, and that the terrorist websites employed significantly more sophisticated multimedia technologies than U.S. government websites.[53]" Perceived anonymity allows for the terrorist member to feel safer, which has allowed their organizations to begin to thrive in cyberspace. According to the CIA, various groups, including al-Qaeda and Hezbollah, are becoming more adept at using the Internet and computer technologies, and these groups could possibly develop the skills necessary for a cyber-attack.[54] This assertion is supported by intelligence that suggests that senior leadership in al-Qaeda has access to the most modern technology equipment. *The Washington Times* has reported that Islamic extremists are calling for the establishment of an Islamist hackers' army to plan cyber-attacks the U.S. government and

[51] Shea, D. A. (2004). *Critical infrastructure: Control systems and the terrorist threat.* ().Congressional Research Service. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467307
[52] Shea, D. A. (2004). *Critical infrastructure: Control systems and the terrorist threat.* ().Congressional Research Service. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467307
[53] *Critical infrastructure: Threats and terrorism.* (10 August 2006). (Handbook No. 1.02). Fort Leavenworth, Kansas: Deputy Chief of Staff for Intelligence (DCSINT). Retrieved from http://www.fas.org/irp/threat/terrorism/sup2.pdf
[54] *Critical infrastructure: Threats and terrorism.* (10 August 2006). (Handbook No. 1.02). Fort Leavenworth, Kansas: Deputy Chief of Staff for Intelligence (DCSINT). Retrieved from http://www.fas.org/irp/threat/terrorism/sup2.pdf

that postings on the extremist bulletin board, al-Farooq, carry detailed cyber-attack instructions, and include spyware programs for download that can be used to learn the passwords of targeted users.[55] It is evident that the strong motivation to attack the United States that is supported by a number of Islamic extremist organizations is materializing into a wide array of potentially dangerous technical capabilities.

State Actors

Just as terrorist organizations remain unrivaled in their desire and expectation to influence a SCADA system, state actors are the leaders when it comes to capabilities in the cyber realm. Therefore, it is vital to identify the state actors that have the strongest desire to attack U.S. critical infrastructure and examine their cyber capabilities accordingly. In today's current geopolitical landscape, Russia and China are the leading threats to the United States from a cybersecurity perspective based on intent and capability. In *An Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Committee on Armed Forces*, National Intelligence Director James Clapper stated, "Among state actors, China and Russia are of particular concern. As indicated in the October 2011 biennial economic espionage report from the National Counterintelligence Executive, entities within these countries are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property.[56]" This section will examine what makes Russia and China the leading state actor-cyber threats to SCADA systems.

[55] *Critical infrastructure: Threats and terrorism.* (10 August 2006). (Handbook No. 1.02). Fort Leavenworth, Kansas: Deputy Chief of Staff for Intelligence (DCSINT). Retrieved from http://www.fas.org/irp/threat/terrorism/sup2.pdf

[56] Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: Director of National Intelligence, Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: (2012).

The Georgian conflict in 2008, the Syrian uprising and the Edward Snowden affair are a few examples of recent instances that have tested and strained U.S.-Russian relations. Tensions between the United States and Russia that have been developing in recent years are currently accelerating due to the situation involving the Ukraine. The foreign policy of Russia's government appears more confident and assertive as its standing on the world stage continues to become more influential. This foreign policy which is promoted by the policy-making elite is characterized by a deep-seated desire to prove to the rest of the world that Russia is in fact a great power that acts independently of the West[57], is shaped in part by internal cyber capabilities, policy and practice.

Russia's cyber warfare doctrine uses offensive cyber weapons as a force multiplier, a military term that describes a weapon or tactic, which significantly increases combat potential when used alongside other military capabilities. Additionally, their cyber strategy emphasizes the ability to disrupt its adversaries' information infrastructure, military and civilian communications and critical infrastructure prior before traditional military operations commence.[58] Moreover, "Russia holds a broad concept of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems and propaganda.[59]" This manifests itself in Russia's larger military doctrine which calls for "prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces.[60]" These objectives make sense considering the current international political climate, where the traditional physical war has

[57] Mankoff, J. (2009). *Russian foreign policy: The return of great power politics*
[58] Kahn, R., McConnell, M., Joseph, N., & Schwartz, P. (2011). America's cyber future.
[59] Smith, D. (2014). Russian cyber capabilities, policy and practice. *The Jewish Policy Center, 8*(1)
[60] Smith, D. (2014). Russian cyber capabilities, policy and practice. *The Jewish Policy Center, 8*(1)

been all but replaced by economic and resource acquisition tactics aimed at gaining leverage in the global scheme. The Russians' relationship with the United States is not a friendly one, and it would be foolish for American leadership to ignore the threats that Russian cyber capabilities could pose against its national security.

A number of factors make Russia a threat in the cyber realm. In his book *Cyber War*, former White House cyber coordinator Richard Clarke writes, "The Russians are definitely better [than China], almost as good as we are…Russian cyber operations are rarely discovered, which is the true measure of a successful op.[61]" In addition to their efforts to win the war of information, Russia's cyber capabilities are bolstered by the factor of corruption, which is the dominant characteristic of their society in a multitude of facets. In Russia, the rule of law that is replaced by personal relationships and payoffs is entirely subjective based on the objectives those who have power. This has spawned a groundswell of state-sponsored, cyber terrorists who have become integrated into the Russian military and conduct strategic espionage against the United States. There are two reasons why Russia sub-contracts some of its cyber work to youth groups and criminals. First it is extremely cost-effective – imagine a reserve force that not only does not cost money, but actually makes money when not employed by the state.[62] Second, use of kids and criminals confounds the attribution problem. Even after extensive cyber forensics, attacks are not traced back to government computers.[63] These corruption tactics not only signify Russia's elevated cyber capabilities, but they also indicate its leadership's desire to, at minimum, win the war of information. The Office of the U.S. National Counterintelligence Executive (NCIX) observes, "Moscow's highly capable intelligence services are using HUMINT (human intelligence), cyber, and other operations to collect economic information and technology to

[61] Smith, D. (2012). Russian cyber operations. *Potomac Institute Cyber Center,*
[62] Smith, D. (2012). Russian cyber operations. *Potomac Institute Cyber Center,*
[63] Smith, D. (2012). Russian cyber operations. *Potomac Institute Cyber Center,*

support Russia's economic development and security.[64]" In addition, there have been recent instances that point towards Russia's intent to undermine the United States, not only from an economic standpoint, but also from a security perspective. In 2009, the *Wall Street Journal* reported that cyber-spies from Russia and China penetrated the U.S. electrical grid, leaving behind software programs. The intruders did not cause damage to U.S. infrastructure, but sought to navigate the systems and their controls.[65] In addition, a Los Angeles water system, an Illinois water pump and a Houston water utility were all reportedly attacked in 2011 by Russian computer hackers.[66] Even more alarmingly, the Houston location was supposedly protected only by a three-letter password. [67] These actions confirm that Russian leadership has both the intent and capabilities to inflict harm on U.S. critical infrastructure, specifically SCADA systems. Russia's extensive attacks on U.S. research and development have resulted in Russia being deemed (along with China), "a national long-term strategic threat to the United States,[68]" by the NCIX.

[64] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*
[65] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*
[66] Blakely, R., & Angeles, L. (2011, November 22). Water system was disabled by russian hackers. *Thetimes.Co.Uk*
[67] Blakely, R., & Angeles, L. (2011, November 22). Water system was disabled by russian hackers. *Thetimes.Co.Uk*
[68] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*

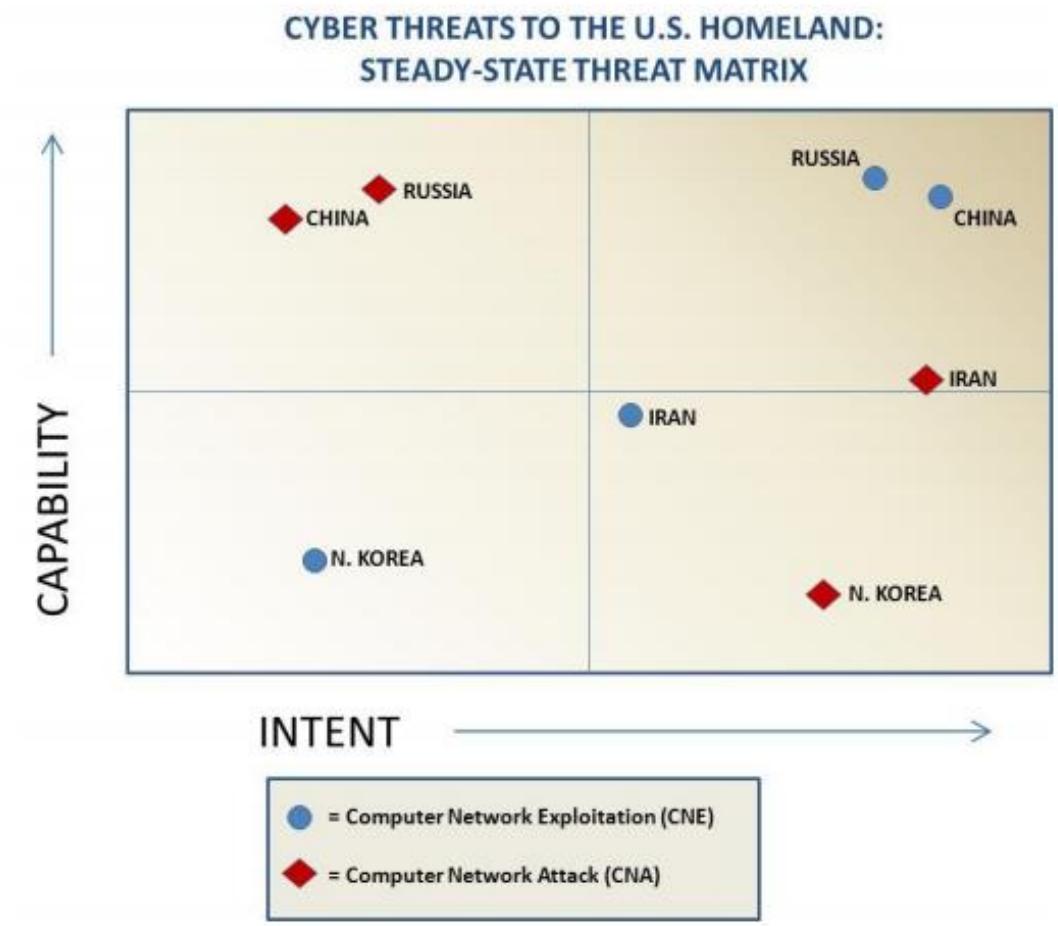

Figure 3: This matrix indicates where Russia and China stand as cyber threats to the United States.[69]

China presents a similar cyber threat to U.S. national security and from an intent perspective; they may be more volatile than the Russians. The Chinese military is over ten years into an expansive military modernization program that has played a tremendous role in the decision-making and identity of the nation's leadership. According to senior American

[69] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*

diplomats, China has the ambition, and increasingly the power, to become a regional hegemon[70], and their government recently announced an 11.2 percent increase in military spending, bringing the total defense budget for 2012 to $106 billion.[71] For a nation that is expected to surpass the U.S. in defense spending in the year 2038, some argue that China is on a collision course to someday collide with the west. This in turn diversifies the capabilities of the People's Liberation Army (PLA), and the Pentagon thinks Chinese leadership is intent on acquiring what is called "anti-access/area denial" capabilities that use pinpoint ground attack and anti-ship missiles, a growing fleet of modern submarines and cyber and anti-satellite weapons to destroy or disable another nation's military assets from afar.[72] However, the extent of China's military capabilities will also be determined by the diplomatic aggressiveness of the government, which American diplomats believe is engaged in a determined effort to lock the U.S. out of the Asia-South Pacific region.[73] Undoubtedly, the Chinese and American governments have experienced friction in recent years, and this friction expands into the cyber realm.

The focus of the Chinese government is characterized by many of the same characteristics in the cyber domain. China relies on black hat programmers to exploit vulnerabilities in external software that has not yet been discovered by the government; but using the underground hacker community is just one of the ways that China is looking to get ahead of the U.S. in the information war. As a part of an integrated national plan, the PLA has adopted a formal cyber warfare doctrine that seeks to attain "electronic dominance" by the year 2050,

[70] The Economist. (2012). The dragon's new teeth. Retrieved 10-3, 2012, from http://www.economist.com/node/21552193

[71] Perelez, J. (2012). Continuing buildup, china boosts military spending more than 11 percent. Retrieved 10-3, 2012, from http://www.nytimes.com/2012/03/05/world/asia/china-boosts-military-spending-more-than-11-percent.html?_r=1

[72] The Economist. (2012). The dragon's new teeth. Retrieved 10-3, 2012, from http://www.economist.com/node/21552193

[73] The Economist. (2012). The dragon's new teeth. Retrieved 10-3, 2012, from http://www.economist.com/node/21552193

which would include targeting its enemies' financial markets, military and civilian communications.[74] It is likely that Chinese leadership is using its maturing computer network exploitation capability to support intelligence collection against the U.S. government and industry by conducting a long term, sophisticated, computer-network exploitation campaign.[75] This campaign has manifested itself in a number of different facets, which have indicated the scope of China's cyber capabilities and the intent of its leadership. It is clear that China possesses sophisticated cyber capabilities and has demonstrated a striking level of perseverance, evidenced by the sheer number of attacks and acts of espionage that the country commits.[76] Additionally, they are widely viewed as an aggressor in cyberspace as the U.S. and other Western nations have identified Beijing as has behind cyber-espionage attempts against their infrastructure computer systems.[77] China's leadership seems to play a large part in the nation's aggressive actions in the global cyber realm. Reports of the Office of the U.S. National Counterintelligence Executive have called out China and its cyber espionage, characterizing these activities as rising to the level of strategic threat to the U.S. national interest. The U.S.-China Economic and Security Review Commission notes further: "Computer network operations have become fundamental to the People's Liberation Army's (PLA) strategic campaign goals for seizing information dominance early in the military operation.[78]" China's efforts appear to be a part of its leadership's larger plan to surpass its adversaries in a number of the primary facets that equate to power on the international stage. China's aggressive collection efforts appear to be

[74] Kahn, R., McConnell, M., Joseph, N., & Schwartz, P. (2011). America's cyber future.
[75] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*
[76] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*
[77] Smithson, S. (2013). China open to cyber-attack. Retrieved 12/9, 2013, from http://www.washingtontimes.com/news/2011/mar/17/china-open-to-cyber-attack/?page=all
[78] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*

intended to amass data and secrets that will support and further the country's economic growth, scientific and technological capacities, military power, etc. – all with an eye to securing strategic advantage in relation to competitor countries and adversaries.[79] With the U.S. being a leading competitor country for the Chinese (and based on their actions that have indicate this as much), it is clear that its leadership has both the intent and capabilities to make China a serious threat to U.S. national security, specifically its critical infrastructure.

[79] Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute,*

VULNERABILITY ANALYSIS

A vulnerability analysis identifies, quantifies and ranks vulnerabilities in a system. Vulnerability is measured through determining two primary factors. First is the attractiveness of the target which can be assessed by the perceived impact that an attack or hindrance would have on a SCADA system. Second is the ease of attack which is evaluated by the significance of the different susceptibilities that might characterize a SCADA system. Understanding the security and vulnerability dynamics behind SCADA systems will help determine how significant SCADA system security is amongst America's national security issues.

Ease of Attack

Within the last fifteen years, SCADA system security has become much more difficult and complex due to their collective transition to Transition Control Protocol/Internet Protocol (TCP/IP) networks, which are the networking models and communication protocols for the Internet. Today, SCADA systems are largely interconnected in order to promote information sharing and efficiency. However, in an industry where the security of industrial control networks was once achieved through physical isolation, the collective transition of SCADA systems to the Internet has made critical infrastructure dangerously susceptible to attack. Thus, critical infrastructure system vulnerability has increasingly been heralded as an emerging national security issue in the United States.

Due to the fundamental role that SCADA systems play in the processing and manipulative functions of many of the critical infrastructure systems in the United States, it is important to review their exposures and liabilities. Considering the move towards

interconnectivity in the critical infrastructure industry, there has been an increased effort to the address the national security concerns that have been surrounding SCADA systems. The weaknesses that plague these systems are numerous and include:

- Staff Experience: With a bent for engineering and technical solutions to problems, the important role of developing security policies can be foreign to a typical SCADA staff, and may therefore not be sympathetic to IT staff recommendations.
- Operating System Vulnerabilities: "SCADA systems are faced with many of the routine IT operating systems susceptibilities, and a bad test and reports of patch-induced problems may cause systems to crash.[80]"
- Authentication: Because it is not uncommon for SCADA systems to possess identical passwords, any sense of authentication and accountability may be lost.[81] Confidentiality of authentication is often compromised by the use of clear text transmissions.
- Remote Access: Because of the economics of staffing control centers around the clock, it is not uncommon for SCADA systems to be configured with remote access, creating another avenue for trespassers to obtain access of the system.
- Interconnectivity: The more connections a system possesses, the more exposure and vulnerability it is susceptible to. "Economic and enterprise pressures often result in an increased volume of internal connections between SCADA systems and partnering constituents.[82]"

[80] Hildick-Smith, N. (2005). Security for critical infrastructure scada systems. Retrieved from http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644
[81] Ten, C., Liu, C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Tranactions on Power Systems, 23*(4)
[82] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001

- Monitoring and Defenses: The use of Intrusion Detection Software (IDS) is not common and firewall and antivirus software has not been a frequent implementation for those in charge of SCADA system security due to staff cutbacks and higher drives for efficiency.
- Wireless: "SCADA systems often use microwave, data radios and cellular packet services for communication, which may present various opportunities for foreign entry, depending on the implementation of the wireless network.[83]"
- Remote Processors: Certain classes of remote processors have been recognized as security vulnerabilities because their computation power and memory resources are diffident and incongruous for security upgrades, as well as the fact that they typically stay in place for ten years or more once they are installed. The result is vulnerable equipment that is not easily or inexpensively replaced.
- SCADA Software: The SCADA application software has modest security features and additional format weaknesses.
- Public Information: It is not uncommon for SCADA system owners to have published papers on the design of their system at a time when security was not a priority; a factor that may eventually breach the security of the system.
- Physical Security: SCADA systems are usually distributed over large distances with multiple unstaffed locations.[84]

These elements are concerning because they collectively extend across the primary control and security components of SCADA systems. When considering the level of ease that an outside attacker could have when accessing a SCADA system, prioritizing its vulnerabilities can

[83] Ten, C., Liu, C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Tranactions on Power Systems, 23*(4)

[84] Hildick-Smith, N. (2005). Security for critical infrastructure scada systems. Retrieved from http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644

be useful. First in regards to networks and remote access, it is important to realize that with current networking technology there can be multiple access points to any network, and physical isolation does not guarantee network security.[85] There is always the possibility of a connection between a local network and the outside world or a connection to another network. This problem multiplies when SCADA system networks are interconnected because of the number of access points available are multiplied. "Over the years, the automation industry has also moved from proprietary standards for SCADA communication protocols towards open international standards, which make it very easy for attackers to gain in-depth knowledge about the working of SCADA networks.[86]" Network protection and interconnectivity concerns are joined by software security as problems that headline SCADA security. SCADA networks utilize commercial-off-the-shelf (COTS) hardware and software, which are cost efficient but sacrifice security. "Devices that are meant to operate in safety-critical environments are usually designed to fail-safe, but security vulnerabilities could be exploited by an attacker to disable to the fail-safe mechanisms.[87]" These vulnerabilities create numerous dangerous possibilities in the event of a cyber-attack on the system. "Attackers aim to compromise the SCADA network's security properties such as integrity, confidentiality, authentication, or availability, and since many of the SCADA protocols do not support any kind of cryptography, sniffing communications on the network are possible if the attacker succeeds in intruding into the network.[88]" Depending on the

[85] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001
[86] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001
[87] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001
[88] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001

level of access that a prospective attacker could gain, there are a number of ways a SCADA system could be manipulated. An attacker could:

- learn all of the data and control commands while listening to the traffic and could use these commands later to send false messages[89];
- tamper with the data transmitted over the network and thereby compromise its integrity[90];
- gain unauthenticated access to devices and change their data set points[91];
- change the operator display values so that when an alarm actually goes off, the human operator is unaware of it, which would delay the response to an emergency[92];
- block or reroute communications to cause significant denial-of-service attacks.[93]

For those concerned with the security of SCADA systems, the problem becomes frustrating knowing that many of these susceptibilities are preventable. For analysts and others who have closely monitored the developing security status of SCADA systems and America's critical infrastructure, the issue of conflicting interests among governmental leadership and the private sector has been a confrontation that has merited substantial attention. The source of the problem is that owners and supervisors of critical infrastructure systems and facilities are chiefly interested in the resources that promote profit; security is not always one of them. SCADA systems brought in $4.6 billion in revenue in 2009 and are expected to rise to nearly $7 billion in

[89] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001
[90] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001
[91] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001
[92] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001
[93] Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001

2016.[94] Because security has not been a primary focus for those who manage vital critical infrastructure systems, vulnerabilities have been pervasive. In addition to the numerous vulnerabilities that hamper SCADA system security, these systems feature virtually no security, firewalls, routers, or antivirus software to protect them.[95] However, this effort to cut corners ultimately deteriorates the overall security of the system itself. Being that nearly 85% of all critical infrastructure is owned and maintained by the private sector, the U.S. government has been challenged with promoting the security and protection of SCADA systems as well as critical infrastructure overall.[96] Cooperation amongst both sides has been a critical subject within both national security and critical infrastructure, and will continue to be a progressing factor towards future security measures.

The Impact of a SCADA System Attack

Evidently, the United States government is faced with a tremendous challenge of protecting American critical infrastructure. The potential impact of a foreign assault on infrastructure elements such as electrical power and communication capabilities of first responders in crises is alarming. The impact of a cyber-attack ranges from network downtime of personal systems to life-threatening destruction of critical infrastructure.[97] Understandably, US critical infrastructure such as financial, electric power and telecommunications may be characterized as the element attracting the greatest threat and possessing the greatest vulnerabilities within the cyber community; based on the potential impact an attack would have

[94] Schwartz, M. J. (2011, April 4). Once invincible, now vulnerable. *Informationweek,* , 8.
[95] Tafoya, W. (2011). Cyber terror. Retrieved 10-3, 2012, from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror
[96] Critical infrastructure: Threats and terrorism. (10 August 2006). (Handbook No. 1.02). Fort Leavenworth, Kansas: Deputy Chief of Staff for Intelligence (DCSINT). Retrieved from http://www.fas.org/irp/threat/terrorism/sup2.pdf
[97] Kahn, R., McConnell, M., Joseph, N., & Schwartz, P. (2011). America's cyber future.

in the way of affecting a large population and causing widespread damage to main pillars of American society.

- *Physical Impacts:* Effects of paramount importance include personal injury or loss of life. Other effects include the loss of property (including data) or damage to the environment. Serious health risks would likely emerge as many American citizens would be without the basic essentials that support function within society. One such result that could contribute to this factor is the elimination of public facilities being able to be utilized. Without electricity primarily, citizens would not have access to resources such as airports, grocery stores, hospitals, fire systems and schools which may further accentuate health problems.
- *Economic Impacts:* Economic impacts are a second-order effect from physical impacts ensuing from cyber intrusion. Physical impacts could result in repercussions to system operations, in which in turn inflict a greater economic loss on the facility or company. On a larger scale, these effects could negatively impact, regional, national, or possibly global economy[98].
- *Social Impacts:* Another second-order effect, the consequence from the loss of national or public confidence in an organization is many times overlooked. It is, however, a very real target and one that can accomplished through a cyber-attack. Widespread panic and paranoia would likely follow after an effective attack on American critical infrastructure. The population may be may constantly be worried about the cleanliness of drinking water

[98] Dillinger, J., Stamp, J., & Young, W. (2003). Common vulnerabilities in critical infrastructure control systems. *Lockheed Martin,*

and the reliability of other government provided services. Social impacts may possibly lead to heavily depressed public confidence or the rise of popular extremism[99].

[99] Dillinger, J., Stamp, J., & Young, W. (2003). Common vulnerabilities in critical infrastructure control systems. *Lockheed Martin,*

Conclusion: Policy Options

Thorough system, threat, and vulnerability assessments have brought forth a number of conclusions with serious national security implications. The SCADA system analysis provided an understanding of what SCADA systems are, what their basic network and control functions include, and how these components interact. The threat analysis indicated that the intent and capabilities of the primary prospective threats to SCADA system security such as hackers and malware, insiders, terrorist organizations, and state actors collectively bring a high level of threat to SCADA system security. The vulnerability analysis indicated that based on the easy-to-moderate level of ease that is required to hack into a SCADA system and the subsequent damage that could possibly ensue in a worst-case scenario, it is evident that SCADA system security is highly vulnerable to attack. With these inferences in mind, it will be vital for analysts and policy makers to be cognizant of the vulnerabilities that characterize SCADA systems and the threats that constantly seek to exploit them.

Solutions:

- As the capabilities and elements of technology continue to become enhanced and developed, it would be beneficial for those faced with the task of upholding the security of SCADA systems to be both adaptable and welcoming in regards to new methodologies of network system security.
- US government engagement with private sector owners and operators of critical infrastructures would help mitigate the threats of cyber terrorism. This solution could be found in the form of more strict governmental security regulations on critical infrastructure systems.

- SCADA system software must be altered with security as a priority. It would advantageous for these systems to possess situational awareness that provides real-time security alerts along with certain solutions to security breaches. This application could be multi-layered across the various zones and sections that constitute system makeup.
- It would be strategic to enhance the regulatory safety mandates that influence and dictate the basic guidelines of American critical infrastructure.
- It would be gainful to implement stricter legal fees, fines and compliance costs for those who do not install and administer proper security measures.

Taking these steps could be the first critical steps towards ensuring that the United States is safe from both external and internal threats in the cyber realm. The potential impact that disrupted critical infrastructure utilities would have on America economically, physically, and socially makes SCADA system security a vital issue. Factoring in the vulnerabilities that characterize SCADA systems and the threats that seek to exploit those weaknesses makes this an issue that merits more attention from our nation's national security leaders.

Bibliography

Bendrath, R. (2001). The cyberwar debate: Perception and politics in US critical infrastructure protection.*7*(Information & Security), 80-103. Retrieved from http://cip.management.dal.ca/publications/Cyberwar%20debate%20-%20perceptions%20and%20politics.pdf

Benjamin, D., & Simon, S. (2000). America and the new terrorism. *Survival, 42*(1), 59-75.

Bergan, C. (2011). Demystifying satellite for the smart grid: Four common misconceptions. Retrieved 12/9, 2013, from http://www.elp.com/articles/powergrid_international/print/volume-16/issue-8/features/demystifying-satellite-for-the-smart-grid-four-common-misconceptions.html

Blakely, R., & Angeles, L. (2011, November 22). Water system was disabled by russian hackers. *Thetimes.Co.Uk*

Cheminod, M. (. 1.)., Pironti, A. (. 2.)., & Sisto, R. (. 2.). (2011). Formal vulnerability analysis of a security system for remote fieldbus access. *IEEE Transactions on Industrial Informatics, 7*(1), 30-40. doi:10.1109/TII.2010.2099233

Cilluffo, F. (2013). Cyber threats from china, Russia and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute*,

CitectSCADA. (2003). Establishing communications and tagging IO devices.*5*(5)

Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: Director of National Intelligence, Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence: (2012).

Critical infrastructure sectors. (2014). Retrieved 4-16, 2013,

Critical infrastructure: Threats and terrorism. (10 August 2006). (Handbook No. 1.02). Fort Leavenworth, Kansas: Deputy Chief of Staff for Intelligence (DCSINT). Retrieved from http://www.fas.org/irp/threat/terrorism/sup2.pdf

Dillinger, J., Stamp, J., & Young, W. (2003). Common vulnerabilities in critical infrastructure control systems. *Lockheed Martin*,

Distler, D.Malware analysis: An introduction. *SAN Institute Reading Room*, Retrieved from http://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103

Epiphan Systems Inc. (2012-2013). Solutions. external SCADA monitoring. Retrieved November 26, 2013, from http://www.epiphan.com/solutions_new/?arid=84

Eusgeld, I., Nan, C., & Dietz, S."System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering and System Safety, 96*, 679-686. doi:10.1016/j.ress.2010.12.010

Ezell, B. C. (2007). Infrastructure vulnerability assessment model (I-VAM). *Risk Analysis: An International Journal, 27*(3), 571-583. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=s3h&AN=25764859&site=eds-live&scope=site

Fieldbus report: Your global source for foundation technology news. (2008).

Galloway, B., & Hancke, G.Introduction to industrial control networks.

Griffith, C. (2012, August 7). Hackers tap into essential services. *The Australian*

Hacking, phishing and malware...OH MY. (2014). Retrieved 2/24, 2014, from https://www.liquidweb.com/blog/index.php/hacking-phishing-and-malware-oh-my/

Hildrick-Smith, A. (2005). Security for critical infrastructure SCADA systems. *SAN Institute Reading Room,*

Igure, V. M., Laughter, S. A., & Williams, R. D.Security issues in SCADA networks. *Computers & Security, 25*, 498-506. doi:10.1016/j.cose.2006.03.001

IHS Global Spec.Trending and historian software information. Retrieved November 26, 2013, from http://www.globalspec.com/learnmore/industrial_engineering_software/industrial_controls_software/trending_historian_software

The jargon file: Hacker slang and hacker culure. Retrieved 2-27, 2014, from http://www.catb.org/jargon/html/introduction.html

Joye, C. (2013, January 9). Brave new world of multi- phase cyber attacks looms. *Australian Financial Review*

Joye, C. (2013, January 2). It's war out there. *Australian Financial Review*

Joye, C. (2013, January 9). Risky business. *Australian Financial Review*

Kahn, R., McConnell, M., Joseph, N., & Schwartz, P. (2011). America's cyber future.

Krekel, B. (2009). Capability of the people's repblic of china to conduct cyber warfare and computer network exploitation. *Northrup Grumman,*

Lawton, S. (2012, January). Hard target: The APT scenario. *SC Magazine (US),*

Lawton, S. (2012, February). New cyber security bill is bipartisan, but has its critics. *SC Magazine (US)*,

Lee, S., Choi, D., Park, C., & Kim, S. (2008). An efficient key management scheme for secure SCADA communication. *Proceedings of World Academy of Science: Engineering & Technology*, *47*, 458-464. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=36317096&site=ehost-live&scope=site

Mankoff, J. (2009). *Russian foreign policy: The return of great power politics*

Marks, E. (2012, April 1). Not in kansas anymore: Securing SCADA. *Embedded Systems Design,* , 11.

McCrady, S. (2013). The elements of SCADA software. *Designing SCADA application software: A practical approach* (pp. 11-23)

McCrady, S. (2013). Practical procedures for SCADA software development.*25*(39)

MEDIATI, N. (2012). 2013 in security: The threats to watch out for. *PC World, 30*(12), 43-44. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=83330901&site=ehost-live&scope=site

Motorola.White paper - SCADA systems.

Munro, K. (2008). SCADA – A critical situation. *Network Security, 2008*(1), 4-6. doi:10.1016/S1353-4858(08)70005-9

Nan, C., Eusgeld, I., & Kröger, W. (2013). Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. *Reliability Engineering & System Safety*, *113*, 76-93. doi:10.1016/j.ress.2012.12.014

O'Harrow, R. (2012). Cyber search engine exposes vulnerabilities. Retrieved 12/9, 2013, from http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html

O'Harrow, R. (2012). Hackers break into energy technology company. Retrieved 12/9, 2013, from http://www.washingtonpost.com/investigations/hackers-break-into-energy-technology-company/2012/09/27/99322e4c-08e6-11e2-a10c-fa5a255a9258_story.html

O'Harrow, R. (2012). Homeland security warns of hackers targeting popular nigeria software. Retrieved 12/9, 2013, from http://www.washingtonpost.com/investigations/homeland-security-warns-of-hackers-targeting-popular-niagara-software/2012/07/13/gJQA0l7NiW_story.html

Patel, S. C., Graham, J. H., & Patricia A.S. Ralston.Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management, 28*, 483-491. doi:10.1016/j.ijinfomgt.2008.01.009

Patel, S. C., & Yu, Y. (2007). Analysis of SCADA security models. *International Management Review, 3*(2), 68-76. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=bth&AN=31672037&site=eds-live&scope=site

Perelez, J. (2012). Continuing buildup, china boosts military spending more than 11 percent. Retrieved 10-3, 2012, from http://www.nytimes.com/2012/03/05/world/asia/china-boosts-military-spending-more-than-11-percent.html?_r=1

Perlroth, N. (2013). Electrical grid is called vulnerable to shutdown. Retrieved 12/5, 2013, from http://bits.blogs.nytimes.com/2013/10/18/electrical-grid-called-vulnerable-to-power-shutdown/?_r=0

Radcliff, D. (2012, November). Waking the sleeping giant: Critical infrastructure. *SC Magazine (US),*

SCADA attack code released for 35 vulnerabilities. (2011, March 23). *Techweb,*

SCADA explained. (2012). *Opus Daytonknight,*

SCADA systems and the terrorist threat : Protecting the nation's critical control systems : Joint hearing before the subcommittee on economic security, infrastructure protection, and cybersecurity with the subcommittee on emergency preparedness, science, and technology of the committee on homeland security, house of representatives, one hundred ninth congress, first session, october 18, 2005 (2007). Washington : U.S. G.P.O. : For sale by the Supt. of Docs., U.S. G.P.O., 2007. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=cat00024a&AN=vmc.b1988891&site=eds-live&scope=site;http://www.lib.jmu.edu/resources/elog.aspx?http://purl.access.gpo.gov/GPO/LPS81409;http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg32242/html/CHRG-109hhrg32242.htm

Schwartz, M. J. (2011, April 4). Once invincible, now vulnerable. *Informationweek,* , 8.

Shea, D. A. (2004). *Critical infrastructure: Control systems and the terrorist threat.* ().Congressional Research Service. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467307

Shin, J., & Spears, D.The basic building blocks of malware.

SIEMENS. (2013). Supervisory control and data acquisition (SCADA). Retrieved 12/9, 2013, from

http://www.water.siemens.com/EN/PRODUCTS/CONTROLS_INSTRUMENTATION_ANALYZERS/SCADA/Pages/default.aspx

Skorobogatjko, A., Dorogovs, P., & Romanovs, A. (2012). The use of intrusion detection systems based on the network behaviour analysis in SCADA networks. *Information Technology & Management Science, ,* 171-175. doi:10.2478/v10313-012-0021-8

Smith, D. (2012). Russian cyber operations. *Potomac Institute Cyber Center,*

Smith, D. (2014). Russian cyber capabilities, policy and practice. *The Jewish Policy Center, 8*(1)

Smithson, S. (2013). China open to cyber-attack. Retrieved 12/9, 2013, from http://www.washingtontimes.com/news/2011/mar/17/china-open-to-cyber-attack/?page=all

Smithson, S. (2013). Feds probing possible cyberattacks at illinois, texas utilities. Retrieved 12/9, 2013, from http://www.washingtontimes.com/news/2011/nov/18/hackers-apparently-based-in-russia-attacked-a-publ/?page=all

Smithson, S. (2013). Hacker group threatens industrial computer systems. Retrieved 12/9, 2013, from http://www.washingtontimes.com/news/2011/oct/17/hacker-group-threatens-industrial-computer-systems/

Spilker, H.Punks, hackers, and unruly technology. *Media and revolt: Strategies and performances from the 1960s to the present* ()

Stouffer, K., Falco, J., & Kent, K.Guide to supervisory control and data acquisition (SCADA) and industrial control systems security.

Tafoya, W. (2011). Cyber terror. Retrieved 10-3, 2012, from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

Ten, C., Liu, C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Tranactions on Power Systems, 23*(4)

The Department of Homeland Security. (2013). Science and technology directorate cyber security division. Retrieved 10/10, 2013, from http://www.dhs.gov/science-and-technology-directorate-cyber-security-division

The Economist. (2012). The dragon's new teeth. Retrieved 10-3, 2012, from http://www.economist.com/node/21552193

Walsh, D. (2013). Cyberstalkers threaten pipeline security. Retrieved 12/8, 2013, from http://green.blogs.nytimes.com/2013/01/10/cyberstalkers-threaten-pipeline-security/

Wang, Y. (2012). sSCADA: Securing SCADA infrastructure communications. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,cpid,uid&custid=s8863137&db=edsarx&AN=1207.5434&site=eds-live&scope=site; http://arxiv.org/abs/1207.5434

Waterman, S. (2011). Hacker group threatens industrial computer systems. Retrieved 2-12, 2014, from http://www.washingtontimes.com/news/2011/oct/17/hacker-group-threatens-industrial-computer-systems/

Weimann, G. (2004). *Cyberterrorism: How real is the threat?* (No. 119). Washington D.C.: United States Institute of Peace. Retrieved from http://dspace.cigilibrary.org/jspui/bitstream/123456789/15033/1/Cyberterrorism%20How%20Real%20Is%20the%20Threat.pdf?1

What is a SCADA system. (2005). Retrieved 12/8, 2013, from http://www.veesta-world.com/pages/services_scada_page.htm

What is malware and how can we prevent it? (2010). Retrieved 2/20, 2014, from http://www.pctools.com/security-news/what-is-malware/

What is the difference: Viruses, worms, trojans, and bots? (2014). Retrieved 2/20, 2014, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

Wilson, C. (2005). *Computer attack and cyberterorism: Vulnerabilities and policy issues for congress.* (No. CRS-2).Congressional Research Service. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a444799.pdf